UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DANIELLE PALLOTTA and CHERYL LAFLAMME, on behalf of themselves and all others similarly situated, Plaintiffs, vs. UNIVERSITY OF MASSACHUSETTS MEMORIAL MEDICAL CENTER and KRONOS INCORPORATED Defendants.	Case No. _____ **COLLECTIVE AND CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Danielle Pallotta ("Ms. Pallotta") and Cheryl Laflamme ("Ms. Laflamme") (collectively, the "Plaintiffs") on behalf of themselves and all others similarly situated (the "Class" or "Class Members"), bring this action against Defendants University of Massachusetts Memorial Medical Center ("UMass Memorial") and Kronos Incorporated ("Kronos") (collectively, the "Defendants") to obtain damages, restitution, and injunctive relief for the Class. Plaintiffs alleges the following based on personal knowledge, the investigation of counsel, and information and belief.

NATURE OF THE ACTION

1. Plaintiffs and Class Members are hourly employees who were not paid the full amount of wages to which they are entitled for all of their work in a timely fashion by UMass Memorial and Kronos.

2. Plaintiffs and Class Members provided their personally identifiable information ("PII") to Defendants at their request, including names, addresses, employee IDs, and social security numbers. Due to UMass Memorial and Kronos' failure to implement and maintain

reasonable safeguards to protect Plaintiffs' PII, criminals obtained access to Plaintiffs' PII, which resulted in substantial harm to Plaintiffs and the Class.[1]

3. This class and collective action seeks to redress Defendants' unlawful withholding of wages for Plaintiffs and Class Members and the negligent disclosure of over 8 million employees' PII in a massive data breach on or around December 11, 2021 ("Data Breach"). On that date, and possibly on others, Defendants' inadequate security measures allowed unauthorized individuals to access and render unusable a workforce management software application Defendants' used to process payroll and store data that contained the PII of Plaintiffs and other individuals.[2]

4. As a result of the Data Breach, Plaintiffs and Class Members were not timely paid the full amount of wages to which they are entitled.

5. Plaintiffs and the Class Members also now bear an immediate and heightened risk of all manners of identity theft. Plaintiffs have incurred, and will continue to incur damages in the form of, *inter alia*, an imminent threat of identity theft, necessary mitigation expenses, loss of privacy and the value of personal information, deprivation of the benefit of the bargain, and/or the additional damages set forth in detail below.

JURISDICTION AND VENUE

6. This Court has personal jurisdiction over Defendant UMass Memorial because it is headquartered in and has its principal place of business in Massachusetts.

7. This Court has personal jurisdiction over Defendant Kronos because it maintains a headquarters in and has its principal place of business in Massachusetts.

---

[1] *See UKG Kronos Community*, Communications Sent to Impact Kronos Private Cloud (KPC) Customers, https://community.kronos.com/s/feed/0D54M00004wJKHiSAO?language=en_US.
[2] *See id.*

8. The FLSA authorizes court actions by private parties to recover damages for violation of the FLSA's wage and hour provisions. 29 U.S.C. § 216(b). Jurisdiction over the FLSA claims asserted herein is based on 29 U.S.C. § 216(b) and 28 U.S.C. § 1331 (federal question jurisdiction). Supplemental jurisdiction over the remaining claims asserted herein exists based upon 28 U.S.C. § 1367.

9. Venue is proper in the District of Massachusetts because, pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to the claims occurred in Massachusetts, and (2) 28 U.S.C. § 1391(b)(1) in that Defendants are residents of Massachusetts.

PARTIES

10. Plaintiff Danielle Pallotta is a resident of Leominster, Massachusetts.

11. Plaintiff Cheryl Laflamme is a resident of Charlton, Massachusetts.

12. On approximately December 11, 2021, Plaintiffs' PII was exposed in the Data Breach. On approximately December 13, 2021, Plaintiffs were not timely paid for the full amount of wages due and their PII was exposed. If Plaintiffs had known that Defendants would not adequately protect their PII, they would not have allowed Defendants access to this sensitive and private information.

13. Defendant Kronos Incorporated is a Delaware Corporation with its principal place of business at 900 Chelmsford St., Lowell, MA 01851.

14. Defendant University of Massachusetts Memorial Medical Center is a not-for-profit corporation with its principal place of business at One Biotech Park, 365 Plantation St., Worcester, MA 01605.

FACTUAL BACKGROUND

A. Plaintiffs' Status As Employees

15. Plaintiffs were employed by UMass Memorial as hourly employees during the relevant time period.

16. During the relevant time period, UMass Memorial was a part of one of the largest health care systems in Massachusetts and employed hourly employees to work in numerous sectors of the health care industry.

17. Plaintiffs' principal job duties included, but were not limited to, providing care for UMass Memorial's patients as registered nurses.

18. Plaintiffs were paid on an hourly basis.

19. UMass Memorial regularly scheduled Plaintiffs' work hours.

20. Plaintiffs regularly reported their hours to UMass Memorial, as instructed by UMass Memorial.

21. UMass Memorial regularly received reports indicating the hours worked by Plaintiffs.

22. On or about December 13, 2021, UMass Memorial instituted a "payment freeze" for all hourly employees, such that the pay for each pay period following that date was set arbitrarily to the period prior to the freeze, with limited exception.

23. UMass Memorial failed to pay Plaintiffs the full amount of wages to which they are entitled for all of their work time in a timely fashion.

24. Plaintiffs made numerous requests for payment of their wages in full, but these requests were denied.

25. Plaintiffs did not furnish their work gratuitously.

26. Plaintiffs worked with the expectation that they would be paid in full for all hours worked in a timely fashion.

27. UMass Memorial did not expect Plaintiffs to perform any work for Defendant gratuitously.

28. Kronos operated and provided a workforce and management software, Kronos Private Cloud, by which UMass Memorial maintained and distributed its payroll to employees.

29. Kronos was acting in the interest of UMass Memorial in relation to Plaintiffs, Class Members, and all employees, by providing this workface and management software.

30. UMass Memorial and Kronos set compensation policies for Plaintiffs and the Class. Defendants were jointly responsible for ensuring that Plaintiffs and the Class were properly paid each pay period. Defendants were also jointly responsible for the unlawful withholding of payments subsequent to the Data Breach.

B. Kronos' Data Breach.

31. Due to inadequate security measures, on or about December 11, 2021, Kronos was the subject of a ransomware attack, whereby criminals obtained access to Plaintiffs' and Class Members PII and Kronos Private Cloud was rendered unusable.[3]

32. Kronos Private Cloud is used by thousands of employers, including UMass Memorial, and 8 million employees to manage work schedules, track hours, and calculate paychecks.[4]

[3] *Id.*
[4] Becky Sullivan, *Hackers disrupt payroll for thousands of employers – including hospitals*, NPR (Jan. 15, 2022), https://www.npr.org/2022/01/15/1072846933/kronos-hack-lawsuits.

33. Kronos and UMass Memorial store employees' PII in Kronos Private Cloud, which can include, *inter alia*, employee names, addresses, employee ID numbers, and social security numbers.[5]

34. The PII of millions of individuals may have been exposed to unauthorized cybercriminals when they gained access to Kronos' server.[6]

35. By disclosing their PII to cybercriminals, Defendants caused Plaintiffs and all Class Members not to timely receive the pay to which they were entitled and put Plaintiffs and all Class Members at risk of identity theft, financial fraud, and other serious harms.

36. Defendants negligently failed to take the necessary precautions required to safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure. Defendants' actions represent a flagrant disregard of Plaintiffs' and the other Class Members' rights, both as to privacy and property.

C. Plaintiffs And Class Members Were Not Paid Proper Wages.

37. Following Kronos' Data Breach, UMass Memorial was unable to operate Kronos Private Cloud and conduct its payroll services.

38. Kronos, through Kronos Private Cloud, maintained control over employee records and the rate and method of payment.

[5] Jennifer Korn, *Kronos ransomware attack could impact employee paychecks and timesheets for weeks*, CNN (Dec. 17, 2021), https://www.cnn.com/2021/12/16/tech/kronos-ransomware-attack/index.html.
[6] *See id*.

39. As a result, numerous employers, including UMass Memorial, who use Kronos Private Cloud for workforce management to manage employee schedules, track hours, and determine payment, were unable to do so.[7]

40. As a result of the Data Breach, Kronos Private Cloud was unable to function properly which restricted the rate and method of payment to employees.

41. UMass Memorial's employees were not paid for the full amount of time they worked in successive pay periods.[8]

42. Plaintiffs and Class Members received payment for far fewer hours than they worked and some Class Members were not paid at all.[9]

43. Some Class Members have been forced to borrow money to pay necessary expenses, including their mortgage or rent.[10]

D. Plaintiffs And Class Members' Personally Identifiable Information Is Valuable.

44. PII is of great value to hackers and cyber criminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners.

45. The term "personally identifiable information" refers to information that can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and biometric records. This can be accomplished alone, or in combination with other

[7] Becky Sullivan, *Hackers disrupt payroll for thousands of employers – including hospitals*, NPR (Jan. 15, 2022), https://www.npr.org/2022/01/15/1072846933/kronos-hack-lawsuits.
[8] Katie Benoit, *Paycheck problems: Following cyber attack, some UMass Memorial Health employees aren't getting paid for correct hours*, SPECTRUM NEWS1 (Jan. 5, 2022), https://spectrumnews1.com/ma/worcester/news/2022/01/05/umass-kronos-paycheck-problems.
[9] Becky Sullivan, *Hackers disrupt payroll for thousands of employers – including hospitals*, NPR (Jan. 15, 2022), https://www.npr.org/2022/01/15/1072846933/kronos-hack-lawsuits.
[10] Katie Benoit, *Paycheck problems: Following cyber attack, some UMass Memorial Health employees aren't getting paid for correct hours*, SPECTRUM NEWS1 (Jan. 5, 2022), https://spectrumnews1.com/ma/worcester/news/2022/01/05/umass-kronos-paycheck-problems.

personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[11]

46. Given the nature of this breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of different ways.

47. A study by Javelin Strategy and Research found that individuals lost about $13 billion in 2020 as a result of identity fraud.[12] Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

48. Indeed, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[13] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[14] Each of these fraudulent activities is difficult to detect. An individual may not know that their Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

49. With access to an individual's PII, cyber criminals can do more than just empty a victim's bank account -- they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the

---

[11] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.
[12] *See Total Identify Fraud Losses Soar to $56 Billion in 2020*, BUSINESSWIRE (Mar. 23, 2021), https://www.businesswire.com/news/home/20210323005370/en/Total-Identity-Fraud-Losses-Soar-to-56-Billion-in-2020.
[13] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1, https://www.ssa.gov/pubs/EN-05-10064.pdf.
[14] *Id*. at 4.

victim's name and social security number to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[15]

E. Defendants Were Aware of the Risk of Cyber-Attacks.

50. Data security breaches -- and data security breach litigation -- dominated the headlines in recent years, including in 2021.[16]

51. UMass Memorial's knowledge of the risks of identity theft is evidenced by its privacy notice:

> UMass Memorial Health Care is required by law to maintain the privacy and security of your medical information, provide this notice of our duties and privacy practices, and abide by the terms of the notice currently in effect. We reserve the right to change privacy practices and make the new practices effective for all the information we maintain. Revised notices will be posted in our facilities, available from your health care provider, and on our web site. We will notify you promptly if a breach occurs that may have compromised the privacy or security of your information.[17]

52. Kronos' knowledge of the risks of identity theft is evidenced by its privacy notice:

> To prevent unauthorized access or disclosure, to maintain data

---

[15] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.

[16] *See e.g.*, Akanksha Rana, *T-Mobile Breach Hits 53 Million Customers as Probe Finds Wider Impact*, REUTERS (Aug. 20, 2021), https://www.reuters.com/technology/t-mobile-says-hackers-accessed-data-another-53-mln-subscribers-2021-08-20/; Jill McKeon, *St. Joseph's/Candler Suffers Ransomware Attack, EHR Downtime*, HEALTHITSECURITY (June 21, 2021), https://healthitsecurity.com/news/st-josephs-candler-suffers-ransomware-attack-ehr-downtime; David E. Sanger, Clifford Krauss, and Nicole Perlroth, *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES (May 8, 2021), https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.

[17] *Joint Notice of Information Practices*, UMASS MEMORIAL HEALTH, https://www.ummhealth.org/patients-visitors/joint-notice-information-practices.

> accuracy, and to allow only the appropriate use of your [personal information], UKG utilizes physical, technical, and administrative controls and procedures to safeguard the information we collect. To protect the confidentiality, integrity, availability and resilience of your PI, we utilize a variety of physical and logical access controls, firewalls, intrusion detection/prevention systems, network and database monitoring, anti-virus, and backup systems. We use encrypted sessions when collecting or transferring sensitive data through our websites. We limit access to your PI and data to those persons who have a specific business purpose for maintaining and processing such information. Our employees who have been granted access to your PI are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided training and instruction on how to do so.[18]

53. The cybercriminals who obtained Class Members' PII may also exploit the PII they obtained by selling the data in the so-called "dark markets." Having obtained these names, addresses, and Social Security numbers, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name.

54. In addition, if a Class Member's Social Security number is used to create a false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the employee's ability to gain employment or obtain a loan.

F. Class Members Have Suffered Concrete Injury as a Result of Defendants' Inadequate Security and the Data Breach It Allowed.

55. Defendants represented to customers that it provided adequate security protections for their PII, and Class Members provided Defendants with sensitive personal information, including their Social Security numbers.

56. The cybercriminals will certainly use Class Members' PII, and Class Members will be at a heightened risk of identity theft for the rest of their lives. Plaintiffs have incurred (and will

[18] Privacy Notice, Ultimate Kronos Group, https://www.ukg.com/privacy#4243725865-507775231.

continue to incur) damages in the form of, *inter alia*, non-payment of wages, loss of privacy and costs of protecting their credit. By this action, Plaintiffs seek to hold Defendants responsible for the harm caused by their negligence.

57. In addition, as a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

58. Defendants' wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[19] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[20] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[21] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. There is also a high probability that criminals who now possess Class Members' PII have not yet used the information, but will do so at a later date or re-sell it.

59. The average cost per customer PII record was $180, based on a study by IBM and the Ponemon Institute.[22] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

---

[19] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267.
[20] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php.
[21] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, http://www.nclnet.org/datainsecurity_report.
[22] *See* Abi Tyas Tunggal, *What Is The Cost of a Data Breach in 2021?*, UPGUARD (Sept. 21, 2021), https://www.upguard.com/blog/cost-of-data-breach.

60. As a result of the Data Breach, Plaintiffs and Class Members have already suffered damages, including, but not limited to, non-payment of wages, imminent threat of identity theft, necessary mitigation expenses, loss of privacy and the value of personal information, and deprivation of the benefit of the bargain.

G. Defendants' Response to the Data Breach Is Inadequate to Protect Class Members.

61. Defendants have failed to provide adequate compensation to Class Members harmed by its negligence. Defendants have not offered credit monitoring for those whose PII was stolen. Defendants have not offered Class Members any assistance in dealing with the IRS or state tax agencies. Nor have Defendants offered to reimburse Class Members for any costs incurred as a result of falsely filed tax returns, a likely consequence of the Data Breach. Nor have Defendants compensated Plaintiffs for injury caused by not receiving timely paychecks or overtime.

COLLECTIVE AND CLASS ACTION ALLEGATIONS

62. Plaintiffs bring Causes of Action I and II as an "opt-in" collective action on behalf of Plaintiffs and similarly situated employees pursuant to 29 U.S.C. § 216(b).

63. Plaintiffs individually and on behalf of other similarly situated employees, seek relief on a collective basis challenging Defendants' practice of failing to pay hourly employees the full amount of wage to which they are entitled for all of their work in a timely fashion.

64. The number and identity of other Plaintiffs yet to opt-in may be ascertained from Defendants' records, and potential class members may be notified of the pendency of this action via mail.

65. Plaintiffs bring this action against Defendants as a collective action on behalf of themselves and all hourly employees of UMass Memorial ("UMass Collective").

66. Plaintiffs and all of the hourly employees are similarly situated in that:

a. Their work has been controlled by UMass Memorial;

b. They have worked as employees of UMass Memorial;

c. They have been economically dependent on UMass Memorial;

d. They regularly reported their hours to UMass Memorial;

e. UMass Memorial regularly received reports indicating the hours worked by Plaintiffs and hourly employees;

f. On or about December 13, 2021, UMass Memorial instituted a "payment freeze" for all hourly employees, such that the pay for each pay period following that date was set arbitrarily to the period that pre-dated freeze, with limited exception for lump sum partial payments of amounts due;

g. UMass Memorial compensated Plaintiffs and many of the collective class members through similar wage rates;

h. On information and belief, other unknown third-parties compensated many class members through similar wage rates;

i. UMass Memorial failed and refused to pay them their full amount of wages.

j. On information and belief, numerous other third parties failed to pay members of the collective who were employed jointly by Kronos and other third parties.

67. Plaintiffs bring this action against Kronos as a collective action on behalf of themselves and all employees who received less than their full wages as a result of the Data Breach ("Kronos Collective").

68. Plaintiffs and all of the hourly employees are similarly situated in that:

a. Their payment and employment records have been controlled by Kronos;

b. They have been economically dependent on Kronos;

c. They regularly reported their hours to Kronos;

d. Kronos regularly received reports indicating the hours worked by Plaintiffs and hourly employees;

e. As a result of the Data Breach, employees' pay for each pay period following the Data Breach was less the amount due for the hours that employees worked;

f. On information and belief, other unknown third-parties compensated many class members through similar wage rates;

g. Kronos' Data Breach is a reason that many employees failed to receive their full amount of wages.

h. On information and belief, numerous other third parties failed to pay members of the collective who used Kronos Private Cloud.

69. Pursuant to Fed. R. Civ. P. 23, Plaintiffs also bring this action against Defendants as a class action on behalf of a Class of all hourly employees of UMass Memorial ("UMass Class").

70. Pursuant to Fed. R. Civ. P. 23, Plaintiffs also bring this action against Kronos as a class action on behalf of a Class of All individuals whose PII was compromised as a result of the Kronos Data Breach announced by Kronos on or about December 11, 2021 ("National Class").

71. Plaintiffs reserve the right to amend the above definition(s), or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

72. Excluded from the Class are Defendants; any parent, subsidiary, or affiliate of Defendants; any entity in which Defendants have or had a controlling interest, or which Defendants otherwise controls or controlled; and any legal representative, predecessor, successor, or assignee of Defendants.

73. This action satisfies the requirements for a class action under F.R.C.P. 23(a)(1) - (a)(4), including requirements of numerosity, commonality, typicality, and adequacy of representation.

74. This action satisfies the requirements for a class action under Rule 23(a)(1). Plaintiffs believes that the proposed Class as described above consists of more than 8 million employees can be identified through Defendants' records, though the exact number and identities of Class Members are currently unknown. The Class is therefore so numerous that joinder of all members, whether otherwise required or permitted, is impracticable.

75. This action satisfies the requirements for a class action under Rule 23(a)(2). Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class Members. Common questions include, but are not limited to, the following:

a. Whether and to what extent Defendants had a duty to protect Class Members' PII;

b. Whether Defendants breached their duty to protect Class Members' PII;

c. Whether Defendants disclosed Class Members' PII;

d. Whether Defendants' conduct was negligent;

e. Whether Plaintiffs and Class Members are entitled to damages; and

f. Whether Defendants' disclosure intruded upon the privacy of Plaintiffs and Class Members.

76. This action satisfies the requirements for a class action under Rule 23(a)(3). The claims asserted by Plaintiffs are typical of the claims of the members of the Class they seek to represent because, among other things, Plaintiffs and Class Members sustained similar injuries as a result of Defendants' uniform wrongful conduct; Defendants owed the same duty to each class member; and Class Members' legal claims arise from the same conduct by Defendants.

77. This action satisfies the requirements for a class action under Rule 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have no interests conflicting with the interests of Class Members. Plaintiffs' Counsel are competent and experienced in data breach class action litigation.

78. Defendants have acted, or refused to act, on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or equitable relief with respect to the Class as a whole.

79. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because Class Members number in the hundreds or thousands and individual joinder is impracticable. Trial of Plaintiffs' and Class Members' claims is manageable. Unless the Class is certified, Defendants will remain free to continue to engage in the wrongful conduct alleged herein without consequence.

80. The prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Defendants.

81. Defendants' wrongful actions, inactions, and omissions are generally applicable to the Class as a whole and, therefore, Plaintiffs also seek equitable remedies for the Class.

82. Defendants' systemic policies and practices also make injunctive relief for the Class appropriate.

83. Absent a class action, Defendants will retain the benefits of its wrongdoing despite its serious violations of the law and infliction of economic damages, injury, and harm on Plaintiffs and Class Members.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Against UMass Memorial On Behalf Of Plaintiffs And The UMass Collective
(Violation Of The FLSA By Failing to Timely Pay Wages)

84. Plaintiffs reassert and re-allege the allegations set forth above.

85. At all times material herein, Plaintiffs and other similarly situated persons have been entitled to the rights, protections, and benefits provided under the FLSA, 29 U.S.C. §§ 201 *et seq*.

86. During all times relevant to this action, UMass Memorial was an "employer" of Plaintiffs within the meaning of the FLSA. 29 U.S.C. § 203(d).

87. During all times relevant to this action, Plaintiffs were UMass Memorial's "employees" within the meaning of the FLSA. 29 U.S.C. § 203(e).

88. Pursuant to the FLSA, employees are entitled to be compensated in a timely manner for their full amount of wages.

89. UMass Memorial violated the FLSA by failing to pay the full amount of wages in a timely manner.

90. Plaintiffs and all similarly situated employees are entitled to damages equal to the difference in the amount of money they were entitled to be paid and the actual amount of money they received.

91. Plaintiffs are entitled to periods of equitable tolling because UMass Memorial acted willfully and knew, or showed reckless disregard for whether its conduct was prohibited by the FLSA, by failing to ensure its payroll and workforce management was equipped to operate correctly in the event of a Data Breach.

92. UMass Memorial has not acted in good faith or with reasonable grounds to believe that its actions and omissions were not a violation of the FLSA, and as a result thereof, the employees are entitled to recover an award of liquidated damages equal to the difference in the amount of money they were entitled to be paid and the actual amount of money they received. Alternatively, should the Court find that UMass Memorial is not subject to an award of liquidated damages, the employees are entitled to an award of prejudgment interest at the applicable legal rate.

93. As a result of the aforesaid willful violations of the FLSA's timely payment requirements, compensation has been unlawfully withheld by UMass Memorial from employees. Accordingly, UMass Memorial is liable under 29 U.S.C. § 216(b), together with an additional

amount as liquidated damages, pre- and post-judgment interest, reasonable attorneys' fees, and costs of this action.

SECOND CAUSE OF ACTION
Against Defendant Kronos On Behalf Of Plaintiffs And The Kronos Collective
(Violation Of The FLSA By Failing to Timely Pay Wages)

94. Plaintiffs reassert and re-allege the allegations set forth above.

95. At all times material herein, Plaintiffs and other similarly situated persons have been entitled to the rights, protections, and benefits provided under the FLSA, 29 U.S.C. §§ 201 *et seq*.

96. During all times relevant to this action, Kronos was an "employer" of Plaintiffs within the meaning of the FLSA because it maintained control over the rate of payment and maintained employment records through Kronos Private Cloud. 29 U.S.C. § 203(d).

97. During all times relevant to this action, Plaintiffs were Kronos' "employees" within the meaning of the FLSA because they were economically dependent on Kronos Private Cloud's operation to receive their full wages. 29 U.S.C. § 203(e).

98. Pursuant to the FLSA, employees are entitled to be compensated in a timely manner for their full amount of wages.

99. Kronos violated the FLSA by failing to pay the full amount of wages in a timely manner.

100. Plaintiffs and all similarly situated employees are entitled to damages equal to the difference in the amount of money they were entitled to be paid and the actual amount of money they received.

101. Plaintiffs are entitled to periods of equitable tolling because Kronos acted willfully and knew, or showed reckless disregard for whether its conduct was prohibited by the FLSA, by

failing to ensure its payroll and workforce management was equipped to operate correctly in the event of a Data Breach.

102. Kronos has not acted in good faith or with reasonable grounds to believe that its actions and omissions were not a violation of the FLSA, and as a result thereof, the employees are entitled to recover an award of liquidated damages equal to the difference in the amount of money they were entitled to be paid and the actual amount of money they received. Alternatively, should the Court find that Kronos is not subject to an award of liquidated damages, the employees are entitled to an award of prejudgment interest at the applicable legal rate.

103. As a result of the aforesaid willful violations of the FLSA's timely payment requirements, compensation has been unlawfully withheld by Kronos from employees. Accordingly, Kronos is liable under 29 U.S.C. § 216(b), together with an additional amount as liquidated damages, pre- and post-judgment interest, reasonable attorneys' fees, and costs of this action.

THIRD CAUSE OF ACTION
Against Defendant Kronos On Behalf Of Plaintiffs And The National Class
(Violation Of Materially Identical State Wage Laws Requiring Timely Payment)

104. Plaintiffs reassert and re-allege the allegations set forth above.

105. Pursuant to the materially identical overtime laws of Massachusetts, New York, Maryland, New Jersey, Ohio, Oregon, Washington, and Washington, D.C., employees are entitled to be compensated at a rate of not less than one and one-half times the regular rate at which such employees are employed for all work performed in excess of 40 hours in a workweek.

106. Kronos violated at least the following materially identical statutes by failing to compensate employees in a timely manner for their full amount of wages:

a. The Massachusetts Wage Act, M.G.L. c. 149, *et seq.*;

b. The New York Labor Law, NYLL §§ 650 *et seq.*;

c. The Maryland Wage and Hour Law; Md. Lab. & Empl. Code §§ 3-415; 3- 420; 3-401(b) & 3-415(a);

d. The New Jersey Wage and Hour Law; N.J.S.A. 34:11–56a *et seq.*;

e. The Ohio Minimum Fair Wage Standard Act, Ohio Rev. Code §§ 4111.03, *et seq.*;

f. The Washington Minimum Wage Act, RCW 49.46.130(1);

g. The District of Columbia Minimum Wage Act, D.C. Code §§ 32-1003(c);

h. The Indiana Wage Payment Statute, Ind. Code § 22-2-5 *et seq.*;

i. The Iowa Wage Payment Collection Law, Iowa Code § 91A.3; and

j. The Rhode Island Payment of Wages Act, Gen. Rhode Island St. § 28-14-1 *et seq.*

107. Plaintiffs and the Collective failed to receive their full amount of wages in a timely manner due to Kronos' Data Breach which uniformly affected all members of the Collective.

108. Plaintiffs and all similarly situated employees are entitled to damages equal to the difference in the amount of money they were entitled to be paid and the actual amount of money they received.

109. Plaintiffs and all similarly situated employees are also entitled to multiple damages as applicable under each state's respective wage law.

110. Plaintiffs are entitled to periods of equitable tolling because Kronos acted willfully and knew, or showed reckless disregard for whether its conduct was prohibited, by failing to ensure its payroll and workforce management was equipped to operate correctly in the event of a Data Breach.

111. Kronos has not acted in good faith or with reasonable grounds to believe that its actions and omissions were not a violation of the materially identical wage statutes, and as a result

thereof, the employees are entitled to recover an award of liquidated damages equal to the difference in the amount of money they were entitled to be paid and the actual amount of money they received. Alternatively, should the Court find that Kronos is not subject to an award of liquidated damages, the employees are entitled to an award of prejudgment interest at the applicable legal rate.

112. As a result of the aforesaid willful violations of the materially identical wage statutes' timely payment requirements, compensation has been unlawfully withheld by Kronos from employees. Accordingly, Kronos is liable, together with an additional amount as liquidated damages, pre- and post-judgment interest, reasonable attorneys' fees, and costs of this action.

FOURTH CAUSE OF ACTION
Against All Defendants On Behalf of The UMass Class
And Against Kronos On Behalf Of The National Class
(Negligence)

113. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

114. Defendants owed a duty to Plaintiffs and to the Class to exercise reasonable care in obtaining, securing, safeguarding, properly disposing of and protecting Plaintiffs and Class Members' sensitive information within its control from being compromised by or being accessed by unauthorized third parties. This duty included, among other things, maintaining adequate control over its computer systems and network so as to prevent unauthorized access thereof.

115. Defendants had full knowledge of the sensitivity of PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were compromised.

116. Defendants had a duty to exercise reasonable care to avoid foreseeable harm in its retention of Plaintiffs' and Class Member's PII.

117. Defendants owed a duty of care to Plaintiffs and members of the Class to provide

security, consistent with industry standards, to ensure that its computer systems adequately protected the sensitive information of the patients in its facilities and networks.

118. Defendants breached its duty of care by failing to secure and safeguard the PII of Plaintiffs and Class Members. Defendants failed to use reasonable measures to protect Class Members' PII. Defendants negligently stored and/or maintained its servers and systems.

119. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiffs' and Class Members' PII would result in injury to Plaintiffs and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members were reasonably foreseeable.

120. It was foreseeable that Defendants knew or should have known that its failure to exercise adequate care in safeguarding and protecting Plaintiffs' and Class Members' PII would result in its release and disclosure to unauthorized third parties who, in turn, wrongfully used such PII or disseminated it for wrongful use.

121. Therefore, it was foreseeable to Defendants that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiffs and Class Members: an imminent threat of identity theft, necessary mitigation expenses, loss of privacy and the value of personal information, deprivation of the benefit of the bargain, ongoing and imminent impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of confidentiality of the stolen confidential data; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; and other economic and non-economic harm.

122. But for Defendants' negligent and wrongful breach of its responsibilities and duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

123. Had Defendants not failed to implement and maintain adequate security measures to protect the PII of its patients, Plaintiffs' and Class Members' PII would not have been exposed to unauthorized access and they would not have suffered any harm.

124. As a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of PII, Plaintiffs and Class Members have incurred, and will continue to incur, the above-referenced damages, and other actual injury and harm.

125. Defendants' wrongful actions, inactions, and omissions constituted (and continues to constitute) common law negligence.

126. Plaintiffs and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

FIFTH CAUSE OF ACTION
Against All Defendants On Behalf of The UMass Class
And Against Kronos On Behalf Of The National Class
(Negligence Per Se)

127. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

128. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect sensitive personal identifying information.

129. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs and Class Members' PII and failing to comply with industry standards.

Defendant's conduct is particularly egregious and unreasonable because of the amount and nature of PII exposed.

130. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

131. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect. In addition, the harm that has occurred is the type of harm the FTC Act was intended to protect against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to maintain and employ reasonable security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Members of the Classes.

132. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have been injured as described above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
Against All Defendants On Behalf Of The National Class
(Violation of Materially Identical State Consumer Protection Statutes)

133. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

134. Plaintiffs and Class Members' PII has been unlawfully exposed without their consent.

135. Defendants engaged in fraudulent or deceptive conduct that creates a likelihood of confusion or of misunderstanding.

136. Defendants knowingly misrepresented and intentionally omitted material information regarding the adequacy of their data security practices.

137. Despite knowledge that their data security measures were unreasonable and

inappropriate, Defendants concealed the fact that employees' PII was not adequately secured.

138. Defendants acted deceptively by failing to inform Plaintiffs and Class Members, who were required to disclose their PII as a condition of their employment, that their PII was not adequately secured.

139. Defendants' conduct directly, foreseeable and proximately caused Plaintiffs and the National Class to suffer an ascertainable loss.

140. The practices discussed above all constitute unfair competition or unfair, unconscionable, deceptive, or unlawful acts or business practices in violation of at least the following state consumer protection statutes:

a. Alaska Unfair Trade Practices and Consumer Protection Act, Alaska Stat. § 45.50.471, *et seq.*;

b. Arizona Consumer Fraud Act, Ariz. Rev. Stat. Ann. § 44-1521, *et seq.*;

c. Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-101, *et seq.*;

d. Connecticut Unfair Trade Practices Act, Conn. Gen Stat. § 42-110a, *et seq.*;

e. Washington D.C. Code § 28-3901, *et seq.*;

f. Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, *et seq.*;

g. Kentucky Consumer Protection Act, Ky. Rev. Stat. Ann. § 367.110, *et seq.*;

h. Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010, *et seq.*;

i. Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1601, *et seq.*;

j. New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 1358-A:1, *et seq.*;

k. New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-1, *et seq.*;

l. New York Deceptive Acts and Practices Act, N.Y. Gen. Bus. Law § 349, *et seq.*;

m. Ohio's Consumers Sales Practice Act, Ohio Revised Code § 1345.01, *et seq.*;

n. Oklahoma Consumer Protection Act, Okla. Stat. tit. 15, § 751, *et seq.*;

o. Rhode Island Unfair Trade Practices and Consumer Protection Act, R.I. Gen. Laws § 6-13.1-1, *et seq.*;

p. Vermont Consumer Fraud Act, Vt. Stat. Ann. Tit. 9 § 2451, *et seq.*; and

q. Washington Consumer Protection Act, Wash. Rev. Code § 19.86.010, *et seq*.

141. Plaintiffs and Class Members are entitled to their actual damages and all other statutory and punitive damages available under these state consumer protection statutes.

142. Plaintiffs and Class Members are further entitled to their costs and reasonable attorney fees.

143. Plaintiffs and Class Members are also entitled to an order enjoining Defendants' unfair, unlawful, and deceptive practices, declaratory relief, and any other necessary or proper relief available under these state consumer protection statutes.

SEVENTH CAUSE OF ACTION
Against All Defendants On Behalf of The UMass Class
And Against Kronos On Behalf Of The National Class
(Intrusion Upon Seclusion/Invasion Of Privacy)

144. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

145. The State of Massachusetts recognizes the right against "unreasonable, substantial or serious interference" with an individual's privacy. M.G.L.A. 214 § 1B.

146. Plaintiffs and the Class Members had a reasonable expectation of privacy in the PII Defendants mishandled.

147. By intentionally failing to keep Plaintiffs' and the Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized

parties for unauthorized use, Defendants intentionally invaded Plaintiffs' and Class Members' privacy by intrusion.

148. Defendants knew that ordinary persons in Plaintiffs' or the Class Members' positions would consider this an invasion of privacy and Defendants' intentional actions highly offensive and objectionable.

149. Defendants invaded Plaintiffs' and the Class Members' right to privacy and intruded into Plaintiffs' and the Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

150. In failing to protect Plaintiffs' and the Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and the Class Members' rights to have such information kept confidential and private.

151. Plaintiffs and the Class Members sustained damages (as outlined above) as a direct and proximate consequence of the invasion of their privacy by intrusion, and therefore seek an award of damages.

NINTH CAUSE OF ACTION
Against All Defendants On Behalf of The UMass Class
And Against Kronos On Behalf Of The National Class
(Breach of Fiduciary Duty)

152. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

153. In providing their PII to Defendants, Plaintiffs and Class Members justifiably placed special confidence in Defendants to act in good faith and with due regard to the interests of Plaintiffs and Class Members in order to safeguard and keep confidential their PII.

154. Defendants accepted the special confidence placed in it by Plaintiffs and Class Members, as evidenced by its assertion stated above in their privacy notices and policies. There was an understanding between the parties that Defendants would act for the benefit of Plaintiffs and Class Members in preserving the confidentiality of the PII.

155. In light of the special relationship between Defendants, Plaintiffs, and the Class Members, whereby Defendants became the guardian of Plaintiffs' and the Class Members' PII, Defendants accepted a fiduciary duty to act primarily for the benefit of its employees, including Plaintiffs and the Class Members. This duty included safeguarding Plaintiffs' and the Class Members' PII.

156. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its employment relationship with its employees, in particular, to keep secure the PII of those employees.

157. Defendants breached their fiduciary duties to Plaintiffs and the Class Members by failing to encrypt and otherwise protect the integrity of its computer systems containing Plaintiffs' and the Class Members' PII.

158. Defendants breached the fiduciary duties they owed to Plaintiffs and the Class Members by failing to timely notify and/or warn them of the Data Breach.

159. Defendants breached their fiduciary duties by failing to ensure the confidentiality and integrity of electronic PII Defendant created, received, maintained, and transmitted.

160. Defendant breached its fiduciary duties by failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights.

161. Defendant breached its fiduciary duties by failing to implement policies and

procedures to prevent, detect, contain, and correct security violations.

162. Defendant breached its fiduciary duties by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity.

163. Defendant breached its fiduciary duties by impermissibly and improperly using and disclosing PII that is and remains accessible to unauthorized persons.

164. Defendant breached its fiduciary duties by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PII.

165. Defendant breached its fiduciary duties by otherwise failing to safeguard Plaintiffs' and the Class Members' Private Information.

166. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class

Members.

167. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

TENTH CAUSE OF ACTION
Against All Defendants On Behalf of The UMass Class
And Against Kronos On Behalf Of The National Class
(Breach of Implied Contract)

168. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

169. Plaintiffs offered services as a condition of employment to Defendants in exchange for monetary payment.

170. As a condition of employment, Defendants required Plaintiffs and Class Members to provide their PII, including names, addresses, dates of birth, Social Security numbers, driver's license numbers, and other personal information. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiffs and Class Members in its possession was only used pursuant to employment.

171. These exchanges constituted an agreement between the parties: Plaintiffs and Class Members would provide their PII and services in exchange for monetary payment provided by Defendants.

172. These agreements were made by Plaintiffs and Class Members who were employees of Defendants.

173. It is clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs and Class Members would not have disclosed their PII to Defendants but for the prospect of Defendant's promise of providing monetary payment for employment. Conversely, Defendants

presumably would not have taken Plaintiffs' and Class Members' PII if it did not intend to provide Plaintiffs and Class Members with monetary payment for employment.

174. Defendants were therefore required to reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure and/or use.

175. Plaintiffs and Class Members accepted UMass Memorial's offer of employment and fully performed their obligations under the implied contract with Defendants by providing services and their PII, directly or indirectly, to Defendants, among other obligations.

176. Plaintiffs and Class Members would not have provided and entrusted their PII to Defendants in the absence of their implied contracts with Defendants and would have instead retained the opportunity to control their PII.

177. Defendants breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII.

178. Defendants' failure to implement adequate measures to protect the PII of Plaintiffs and Class Members violated the purpose of the agreement between the parties.

179. Defendants were on notice that its systems and data security protocols were inadequate yet failed to invest in the proper safeguarding of Plaintiffs' and Class Members' PII, which Plaintiffs and Class Members were required to provide to Defendants.

180. As a proximate and direct result of Defendants' breaches of its implied contracts with Plaintiffs and Class Members, Plaintiffs and the Class Members suffered damages as described in detail above.

ELEVENTH CAUSE OF ACTION
Against All Defendants On Behalf of The UMass Class
And Against Kronos On Behalf Of The National Class
(Breach of Covenant of Good Faith and Fair Dealing)

181. Plaintiffs re-allege and incorporate by reference all paragraphs above as if

fully set forth herein.

182. As described above, when Plaintiffs and Class Members provided their PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect Plaintiffs' and Class Members' PII and to timely detect and notify them in the event of a data breach.

183. These exchanges constituted an agreement between the parties: Plaintiffs and Class Members were required to provide their PII as a condition of employment, as well as an implied covenant by Defendant to protect Plaintiffs' PII in its possession.

184. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs and Class Members would not have disclosed their PII to Defendants but for the prospect of Defendants' promise of monetary compensation for employment. Conversely, Defendants presumably would not have taken Plaintiffs' and Class Members' PII if it did not intend to provide Plaintiffs and Class Members with monetary compensation for employment.

185. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiffs and Class Members in its possession was only used for payroll purposes.

186. While Defendants had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

187. Defendants breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' PII and failing to disclose to Plaintiffs and Class Members at the time they provided their PII to it that

Defendants data security systems failed to meet applicable legal and industry standards.

188. Plaintiffs and Class Members did all or substantially all the significant things that the contract required them to do.

189. Likewise, all conditions required for Defendants' performance were met.

190. Defendants' acts and omissions unfairly interfered with Plaintiffs' and Class Members' rights to receive the full benefit of their contracts.

191. Plaintiffs and Class Members have been or will be harmed by Defendants' breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

192. Defendants are liable for their breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

193. Plaintiffs and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

TWELFTH CAUSE OF ACTION
Against All Defendants On Behalf of The UMass Class
And Against Kronos On Behalf Of The National Class
(Declaratory and Injunctive Relief)

194. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

195. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

196. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendants to provide adequate security for the PII it collected from

Plaintiffs and Class Members.

197. Defendants owe a duty of care to Plaintiffs and Class Members requiring it to adequately secure their PII.

198. Defendants still possesses Plaintiffs' and Class Members' PII.

199. Since the Data Breach, Defendants have announced few, if any, changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

200. Defendants have not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendants' insufficient data security is known to hackers, the PII in Defendants' possession is even more vulnerable to cyberattack.

201. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendants' failure to address the security failings that led to such exposure.

202. There is no reason to believe that Defendants' security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

203. Plaintiffs, therefore, seeks a declaration (1) that Defendants' existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendants segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

f. Ordering that Defendants conduct regular computer system scanning and security checks;

g. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendants to meaningfully educate its current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, respectfully request that the Court grant relief against Defendant as follows:

A. For an Order certifying that this action may be prosecuted as a collective action pursuant to the FLSA and requiring notice thereto to be paid by Defendants;

B. Certifying this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and requiring notice thereto to be paid by Defendants;

C. Appointing Plaintiffs and their counsel to represent the Class;

D. For appropriate injunctive relief and/or declaratory relief, including an Order requiring Defendants to immediately secure and fully encrypt all confidential information, to properly secure computers containing confidential information, to cease negligently storing, handling, and securing its Employees' confidential information, and to provide identity theft monitoring for an additional five years;

E. Adjudging and decreeing that Defendants have engaged in the conduct alleged herein;

F. For compensatory and general damages according to proof on certain causes of action;

G. For reimbursement, restitution, and disgorgement on certain causes of action;

H. For both pre- and post-judgment interest at the maximum allowable rate on any amounts awarded;

I. For costs of the proceedings herein;

J. For an Order awarding Plaintiffs and the Class reasonable attorney's fees and expenses for the costs of this suit;

K. Trial by jury; and

L. For any and all such other and further relief that this Court may deem just and proper, including but not limited to punitive or exemplary damages.

Dated: March 9, 2022
White Plains, NY

Respectfully Submitted,

FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP

By: */s/ D. Greg Blankinship*
D. Greg Blankinship (Mass. Bar #655430)
Jeremiah Frei-Pearson (*pro hac vice* application forthcoming)
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
gblankinship@fbfglaw.com
jfrei-pearson@fbfglaw.com

Attorneys for Plaintiffs and the Proposed Collectives and Classes